

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system to enforce privacy preferences on exchanges of personal data of a data-subject, the system comprising of one or more computers connected to one or more networks through one or more network interfaces, each computer having one or more memories and one or more central processing units (CPUs), the system further comprising:

one or more data-subject authorization rule sets stored in the one or more memories that has one or more subject constraints on release of one or more private, subject data-subject data-releases;

a receiving process, executing on the one or more CPUs, that receives a request message from a data-requester requester over the network interfaces, the request message having one or more requests for one or more of the private, subject data-subject data releases pertaining to a subject, and a requester privacy statement for each of the respective private data-subject data requested, wherein the requester privacy statement describes how each of the requested data-subject data will be used by the requester; and

a release process executing on the one or more CPUs that compares the requester privacy statement to the subject constraints and releases the private, subject

data-subject data release in a response message to the requester only if the subject constraints are satisfied.

2. (Currently Amended) A system, as in claim 1, where the requester also has to be authorized to receive the private data-subject data.

3. (Original) A system, as in claim 2, where there is more than one level of authorization.

4. (Currently Amended) A system, as in claim 1, wherein each of the subject constraints further comprises:

an authorization dataset describing the data-subject data to which the subject constraint applies;

a privacy preference rule that describes the privacy preferences under which the data-subject data may be released and the corresponding actions allowed;

an access list describing who is allowed to access the data-subject data; and

an authorization action that describes any additional action to be taken if the restrictions imposed by the authorization dataset, the privacy preference rule and the access list of this constraint are matched.

5. (Currently Amended) A system, as in claim 1, wherein the private, subject data-subject data release further comprises:

one or more subject data that is owned and held by the data-subject;

one or more subject data that is owned by the data-subject, but held by one or more parties on behalf of the ~~data~~-subject data-subject; and

one or more subject data that is owned and held by one or more third parties.

6. (Currently Amended) A system, as in claim 1, where one or more of the requesters have to satisfy different data-subject authorization rule sets for the same private data-subject data.

7. (Currently Amended) A system, as in claim 1, where the private, subject data-subject data release is partitioned into a first part that satisfies the subject constraints and is released and a second part that does not satisfy the subject constraints and is not released.

8. (Currently Amended) A system, as in claim 1, wherein the private, subject data-subject data released further comprises one or more data for which additional manual authorization from the data-subject is needed before the data is released.

9. (Currently Amended) A system, as in claim 1, wherein the private, subject data-subject data released further comprises one or more missing values which have to be acquired from the data-subject before the data-subject data is released.

10. (Currently Amended) A system, as in claim 1, wherein private, subject data-subject data released further comprises one or more data that is stored with one or

more third parties and has to be retrieved from the third parties before the ~~private~~,
~~subject~~ data-subject data release can be released.

11. (Currently Amended) A system, as in claim 1, wherein the ~~private~~, ~~subject~~ data-subject data released further comprises one or ~~ore~~ more data that is stored with one or more third parties and the third parties have to be provided with authorization to release the data to the requester.

12. (Currently Amended) A system, as in claim 1, where the ~~private~~, ~~subject~~ data-subject data release to which each constraint applies comprises one or more of the following: one or more classes of data, one or more properties of data, and one or more instances of data.

13. (Currently Amended) A system, as in claim 1, where the ~~private~~, ~~subject~~ data-subject data release is ordered in a hierarchy with one or more levels and each of the levels has one or more constraints that apply to the respective ~~private~~, ~~subject~~ data-subject data release in the level.

14. (Original) A system, as in claim 13, where one or more of the levels have different constraints.

15. (Original) A system, as in claim 13, where one or more of the levels inherits one or more of the constraints from one or more other levels.

16. (Original) A system, as in claim 13, where the level to which each constraint applies further comprises one or more of the following: one or more classes of data, one or more properties of data, and one or more instances of data.

17. (Currently Amended) A system, as in claim 1, where the subject constraints include privacy preferences based on any one or more of the Platform for Privacy Preferences (P3P) standard privacy statements, including a purpose, a retention, a recipient and an access.

18. (Currently Amended) A system, as in claim 1, where the data-subject data includes any one or more of the following: a privacy data, a privacy data associated with a natural person, a confidential information, and a trade secret.

19. (Currently Amended) A method to enforce privacy preferences on exchanges of personal data of a data-subject, comprising the steps of:

specifying one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints on one or more private, subject data-subject data-releases;

receiving a request message from a data-requester-requester, the request message having one or more requests for one or more of the data-subject data releases pertaining to the a subject, and a requester privacy statement for each of the respective private, subject data-subject data release requested, wherein the requester privacy

statement describes how each of the requested data-subject data will be used by the requester;

comparing the requester privacy declaration statement to the subject constraints; and

releasing the private, subject data-subject data release in a response message to the requester only if the subject constraints are satisfied.

20. (Currently Amended) The method of claim 19, further comprising the step of authorizing the requester to receive the private, subject data-subject data-release.

21. (Original) The method of claim 20, wherein the step of authorizing the requester includes the steps of authorization at more than one level.

22. (Currently Amended) The method of claim 19, wherein the step of specifying each of the one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of:

specifying an authorization dataset describing the data to which the constraint applies;

specifying a privacy preference rule that describes the privacy preferences under which the private, subject data-subject data release may be released and the corresponding actions allowed;

specifying an access list describing who is allowed to access the said data; and

specifying an authorization action that describes any additional action to be taken if the restrictions imposed by the authorization dataset, the privacy preference rule and the access list of this constraint are matched.

23. (Currently Amended) The method of claim 19, wherein the step of specifying each of the one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of:

specifying such constraints for subject data that owned and held by the subject;
specifying such constraints for ~~private, subject~~ data-subject data that is owned by the data subject, but held by one or more parties on behalf of the subject; and
specifying such constraints for ~~private subject~~ data-subject data that is owned and held by one or more third parties.

24. (Currently Amended) The method of claim 19, wherein the step of specifying each said one or more data-subject authorization rule sets includes the steps of specifying different data-subject authorization rule sets for the same ~~private~~ data-subject data for one or more requesters that must be satisfied for them to get the ~~private, subject~~ data-subject data to be released.

25. (Currently Amended) The method of claim 19, wherein the step of comparing the requester privacy declaration statement to the subject constraints includes the step of partitioning the private data-subject data into a first part that satisfies the constraints

and is released and a second part that does not satisfy the constraints and is not released.

26. (Currently Amended) The method of claim 19, wherein the step of releasing the data-subject data includes the step of getting manual authorization from the data-subject for some of the data-subject data before releasing the data.

27. (Currently Amended) The method of claim 19, wherein the step of releasing the data-subject data includes the step of getting one or more missing values from the data-subject before releasing the data.

28. (Currently Amended) The method of claim 19, wherein the step of releasing the data-subject data includes the step of getting one or more data-subject data from one or more third parties, that store that data-subject data, before releasing the data.

29. (Currently Amended) The method of claim 19, wherein the step of releasing the data includes the step of providing authorization to one or more third parties holding part of the private, subject data-subject data release to release the part to the requester.

30. (Currently Amended) The method of claim 19, wherein the step of specifying each of the one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of:
ordering the data-subject data in a hierarchy with one or more levels; and

specifying one or more constraints for each level that apply to the data-subject data in that level.

31. (Currently Amended) The method of claim 19, wherein the step of specifying each said subject constraint includes the step of specifying one or more of the following: one or more classes of data, one or more properties of data, and one or more instances of data.

32. (Original) The method of claim 30, wherein the step of specifying constraints for each level includes the step of specifying different constraints for one or more of the levels.

33. (Original) The method of claim 30, wherein the step of specifying constraints for each level includes the step of inheriting the constraints from one or more other levels.

34. (Currently Amended) The method of claim 30, wherein the step of ordering the data-subject data into a hierarchy of levels includes the step of creating levels from one or more classes of data, properties of data, instances of data, or a combination thereof these.

35. (Currently Amended) The method of claim 19, wherein the step of specifying each said one or more data-subject authorization rule sets, the data-subject

authorization rule set having one or more subject constraints includes the steps of specifying constraints that include privacy preferences based on any one or more of a Platform for Privacy Preferences (P3P) standard privacy statements.

36. (Original) A method, as in claim 35 where the standard privacy statements include any one or more of the following: a purpose, a retention, a recipient and an access.

37. (Currently Amended) The method of claim 19, wherein the step of specifying each said one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of specifying constraints over subject data that includes any one or more of the following: a privacy data, a privacy data associated a natural person, a confidential information, and a trade secret.

38. - 47 (Withdrawn)